27001:2013 Audit Checklist

Company Name:

Audit Date:

Auditor:

### Attendees

|  |  |
| --- | --- |
| Opening meeting  | Closing meeting |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Note: You should confirm that mandatory documentation exists and appears appropriate and adequate. You should ensure that audits and management reviews are being conducted, although a comprehensive review is not required at this stage. You are not required to complete all of the sections below, but they are made available for use as applicable.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **4** | **Context of the organization** |  |  |  |  |  |  |
| 4.1 | Understanding the organization and its context  |  |  |  |  |  |  |
|  | Has the organization determined the external and internal issues that are relevant to its purpose?Give details of these.  |  |  |  |  |  |  |
|  | Has the organization determined the external and internal issues that affect its ability to achieve the intended outcome(s) of its information security management system?Give details of these. |  |  |  |  |  |  |
| 4.2 | Understanding the needs and expectations of interested parties |  |  |  |  |  |  |
|  | Has the organization identified the interested parties that are relevant to its information security management system?Give details of these. |  |  |  |  |  |  |
|  | Has the organization determined the requirements of the interested parties who are relevant to its information security management system?Give details of these. |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 4.3 | Determining the scope of the information security management system |  |  |  |  |  |  |
|  | Has the organization determined the boundaries and applicability of its information security management system when establishing its scope? |  |  |  |  |  |  |
|  | When determining its scope has the organization considered the external and internal issues referred to in 4.1 and how these are to be achieved? |  |  |  |  |  |  |
|  | When determining its scope has the organization considered the requirements referred to in 4.2? |  |  |  |  |  |  |
|  | When determining its scope has the organization considered the interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations? |  |  |  |  |  |  |
|  | Is the scope available as documented information? |  |  |  |  |  |  |
| 4.4 | Information security management system |  |  |  |  |  |  |
|  | Has the organization established, implemented, maintained and continually improved an information security management system, in accordance with the requirements of ISO 27001:2013? |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **5** | **Leadership** |  |  |  |  |  |  |
| 5.1 | Leadership and commitment |  |  |  |  |  |  |
|  | Has top management demonstrated leadership and commitment with respect to the information security management system by ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization? |  |  |  |  |  |  |
|  | Has top management demonstrated leadership and commitment with respect to the information security management system by ensuring the integration of the information security management system requirements into the organization’s processes? |  |  |  |  |  |  |
|  | Has top management demonstrated leadership and commitment with respect to the information security management system by ensuring that the resources needed for the information security management system are available? |  |  |  |  |  |  |
|  | Has top management demonstrated leadership and commitment with respect to the information security management system by communicating the importance of effective information security management and of conforming to the information security management system requirements? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Has top management demonstrated leadership and commitment with respect to the information security management system by ensuring that the information security management system achieves its intended outcome(s)? |  |  |  |  |  |  |
|  | Has top management demonstrated leadership and commitment with respect to the information security management system by directing and supporting persons to contribute to the effectiveness of the information security management system? |  |  |  |  |  |  |
|  | Has top management demonstrated leadership and commitment with respect to the information security management system by supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility? |  |  |  |  |  |  |
| 5.2 | Policy |  |  |  |  |  |  |
|  | Has top management established an information security policy that is appropriate to the purpose of the organization? |  |  |  |  |  |  |
|  | Has top management established an information security policy that includes information security objectives or provides the framework for setting information security objectives? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Has top management established an information security policy that includes a commitment to satisfy applicable requirements related to information security? |  |  |  |  |  |  |
|  | Has top management established an information security policy that includes a commitment to continual improvement of the information security management system? |  |  |  |  |  |  |
|  | Is the information security policy available as documented information that is communicated within the organization? |  |  |  |  |  |  |
|  | Is the information security policy available to interested parties, as appropriate? |  |  |  |  |  |  |
| 5.3 | Organizational roles, responsibilities and authorities |  |  |  |  |  |  |
|  | Does top management ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated? |  |  |  |  |  |  |
|  | Has top management assigned the responsibility and authority for ensuring that the information security management system conforms to the requirements of ISO 27001:2013?Give details of person/function within the organization. |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Has top management assigned the responsibility and authority for reporting on the performance of the information security management system to top management?Give details of person/function within the organization. |  |  |  |  |  |  |
|  | Information security policies |  |  |  |  |  |  |
|  | Are the policies for information security reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness?Give details. |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **6**  | **Planning** |  |  |  |  |  |  |
|  | Has the organization a mobile device policy based on risk assessment? |  |  |  |  |  |  |
|  | Has the organization a teleworking policy based on risk assessment? |  |  |  |  |  |  |
|  | Have risk assessments defined security responsibilities and from these allocated them appropriately? |  |  |  |  |  |  |
|  | Are conflicting duties and areas of responsibility segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets? |  |  |  |  |  |  |
|  | Is information security addressed in project management, regardless of the type of the project? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 6.1 | Actions to address risks and opportunities |  |  |  |  |  |  |
| 6.1.1  | General |  |  |  |  |  |  |
|  | When planning the information security management system has the organization considered the issues referred to in 4.1 and the requirements referred to in 4.2? |  |  |  |  |  |  |
|  | When planning the information security management system has the organization determined the risks and opportunities that need to be addressed?Please list identified risks and opportunities. |  |  |  |  |  |  |
|  | When planning the information security management system has the organization ensured that it can achieve its intended outcome(s)? |  |  |  |  |  |  |
|  | When planning the information security management system has the organization ensured that it can prevent, or reduce, undesired effects? |  |  |  |  |  |  |
|  | When planning the information security management system has the organization ensured that it can achieve continual improvement? |  |  |  |  |  |  |
|  | Does the organization plan actions to address these risks and opportunities? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Does the organization plan actions to address how to integrate and implement the actions into its information security management system processes? |  |  |  |  |  |  |
|  | Does the organization plan actions to address how to evaluate the effectiveness of these actions? |  |  |  |  |  |  |
| 6.1.2 | Information security risk assessment |  |  |  |  |  |  |
|  | Has the organization defined and applied an information security risk assessment process? |  |  |  |  |  |  |
|  | Has the information security risk assessment process established and maintained information security risk criteria? |  |  |  |  |  |  |
|  | Do such security risk criteria cover risk acceptance and criteria for performing information security risk assessments?Give details. |  |  |  |  |  |  |
|  | Does the risk assessment process ensure that repeated information security risk assessments produce consistent, valid and comparable results? |  |  |  |  |  |  |
|  | Does the risk assessment identify the information security risks that apply to the process for identifying risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system?  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Does the risk assessment process identify the risk owners? |  |  |  |  |  |  |
|  | Does the risk assessment process analyses the information security risks? |  |  |  |  |  |  |
|  | Does the risk assessment process assess the potential consequences that would result if the risks are identified or were to materialize? |  |  |  |  |  |  |
|  | Does the risk assessment process assess the realistic likelihood of the occurrence of the risks identified and determine the levels of risk? |  |  |  |  |  |  |
|  | Does the risk assessment process evaluate the information security risks? |  |  |  |  |  |  |
|  | Does the risk assessment process compare the results of risk analysis with the risk criteria established and prioritize the analysed risks for risk treatment? |  |  |  |  |  |  |
|  | Does the organization retain documented information about the information security risk assessment process? |  |  |  |  |  |  |
| 6.1.3 | Information security risk treatment |  |  |  |  |  |  |
|  | Has the organization defined and applied an information security risk treatment process to select appropriate information security risk treatment options, taking account of the risk assessment results? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Has the organization determined all controls that are necessary to implement the information security risk treatment option(s) chosen? |  |  |  |  |  |  |
|  | Has the organization compared the controls required and verify that no necessary controls have been omitted? |  |  |  |  |  |  |
|  | Has the organization produced a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls? |  |  |  |  |  |  |
|  | Has the organization formulated an information security risk treatment plan? |  |  |  |  |  |  |
|  | Has the organization obtained risk owners’ approval of the information security risk treatment plan and acceptance of the residual information security risks? |  |  |  |  |  |  |
| 6.2 | Information security objectives and planning to achieve them |  |  |  |  |  |  |
|  | Has the organization established information security objectives at relevant functions and levels? |  |  |  |  |  |  |
|  | Are the information security objectives consistent with the information security policy? |  |  |  |  |  |  |
|  | Are the information security objectives measurable (if practicable)? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Do the information security objectives take into account applicable information security requirements, and results from risk assessment and risk treatment? |  |  |  |  |  |  |
|  | Are the information security objectives communicated; and updated as appropriate? |  |  |  |  |  |  |
|  | Does the organization retain documented information on the information security objectives? |  |  |  |  |  |  |
|  | When planning how to achieve its information security objectives does the organization determine what will be done? |  |  |  |  |  |  |
|  | When planning how to achieve its information security objectives does the organization determine what resources will be required? |  |  |  |  |  |  |
|  | When planning how to achieve its information security objectives does the organization determine who will be responsible? |  |  |  |  |  |  |
|  | When planning how to achieve its information security objectives does the organization determine when it will be completed and how the results will be evaluated? |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **7** | **Support** |  |  |  |  |  |  |
|  | Does the organization have details of knowledge held by it including qualification and reference materials? |  |  |  |  |  |  |
|  | When carrying out risk assessments is organizational knowledge a factor considered? |  |  |  |  |  |  |
|  | Does the organization carry out background verification checks on all candidates for employment in accordance with relevant laws, regulations and ethics which are proportional to the business requirements, the classification of the information to be accessed and the perceived risks? |  |  |  |  |  |  |
|  | Do the contractual agreements with employees and contractors state their and the organization’s responsibilities for information security? |  |  |  |  |  |  |
|  | Does management require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization? |  |  |  |  |  |  |
|  | Do all employees of the organization and, where relevant, contractors receive appropriate awareness education and trainingand regular updates in organizational policies and procedures, as relevant for their job function? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Is there a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach? |  |  |  |  |  |  |
|  | Are information security responsibilities and duties that remain valid after termination or change of employment defined, communicated to the employee or contractor and enforced? |  |  |  |  |  |  |
| 7.1 | Resources |  |  |  |  |  |  |
|  | Has the organization determined and provided the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system? |  |  |  |  |  |  |
| 7.2 | Competence |  |  |  |  |  |  |
|  | Has the organization determined the necessary competence of person(s) doing work under its control that affects its information security performance? |  |  |  |  |  |  |
|  | Does the organization ensure that these persons are competent on the basis of appropriate education, training, or experience? |  |  |  |  |  |  |
|  | Does the organization retain appropriate documented information as evidence of competence? |  |  |  |  |  |  |
| 7.3 | Awareness |  |  |  |  |  |  |
|  | Are persons doing work under the organization’s control aware of the information security policy? |  |  |  |  |  |  |
|  | Are persons doing work under the organization’s control aware of their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance? |  |  |  |  |  |  |
|  | Are persons doing work under the organization’s control aware of the implications of not conforming with the information security management system requirements?Give details of these consequences of not complying. |  |  |  |  |  |  |
| 7.4 | Communication |  |  |  |  |  |  |
|  | Has the organization determined the need for internal and external communications relevant to the information security management system? |  |  |  |  |  |  |
|  | Do the above include what to communicate; when to communicate; with whom to communicate; who shall communicate and the processes by which communication shall be effected? |  |  |  |  |  |  |
|  | Have the above been taken into account when risk assessing the communication process? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 7.5 | Documented Information |  |  |  |  |  |  |
|  | NOTE: The extent of documented information for an information security management system can differ from one organization to another due to:1. the size of organization and its type of activities, processes, products and services;
2. the complexity of processes and their interactions; and
3. the competence of persons.
 |  |  |  |  |  |  |
| 7.5.1 | General |  |  |  |  |  |  |
|  | Does the organization’s information security management system shall include documented information required by ISO 27001:2013? |  |  |  |  |  |  |
|  | List document that form the system, both mandatory and optional. (identify Mandatory with a prefix M) |  |  |  |  |  |  |
|  | Has the documented information determined by the organization as being necessary for the effectiveness of the information security management system been verified as such by competent members of the organization?. |  |  |  |  |  |  |
| 7.5.2 | Creating and updating |  |  |  |  |  |  |
|  | When creating and updating documented information does the organization ensure appropriate identification and description (e.g. a title, date, author, or reference number)? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | When creating and updating documented information does the organization ensure consistency in format (e.g. language, software version, graphics) and media (e.g. paper, electronic)? |  |  |  |  |  |  |
|  | When creating and updating documented information do assigned competent members of the organization review and approve them for suitability and adequacy? |  |  |  |  |  |  |
| 7.5.3 | Control of documented information |  |  |  |  |  |  |
|  | Is documented information required by the information security management system adequately controlled to ensure it is available and suitable for use, where and when it is needed? |  |  |  |  |  |  |
|  | Is documented information required by the information security management system adequately controlled to ensure it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity)?  |  |  |  |  |  |  |
|  | For the control of documented information, does the organization address the following activities,as applicable:1. distribution, access, retrieval and use;
2. storage and preservation, including the preservation of legibility;
3. control of changes (e.g. version control); and
4. retention and disposition.
 |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Is documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system identified as appropriate, and controlled? |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 8 | Operation |  |  |  |  |  |  |
|  | Are assets associated with information and information processing facilities identified and an inventory of these assets drawn up and maintained? |  |  |  |  |  |  |
|  | Are assets maintained in the inventory owned by individual members of the organization to allow for identification? |  |  |  |  |  |  |
|  | Are rules for the acceptable use of information and of assets associated with information and information processing facilities identified, documented and implemented? |  |  |  |  |  |  |
|  | Do all employees and external party users return all of the organizational assets in their possession upon termination of their employment, contract or agreement? |  |  |  |  |  |  |
|  | Is information classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Has an appropriate set of procedures for information labelling been developed and implemented in accordance with the information classification scheme adopted by the organization? |  |  |  |  |  |  |
|  | Have procedures for handling assets been developed and implemented in accordance with the information classification scheme adopted by the organization? |  |  |  |  |  |  |
|  | Are procedures implemented for the management of removable media in accordance with the classification scheme adopted by the organization? |  |  |  |  |  |  |
|  | Is media disposed of securely when no longer required, using formal procedures? |  |  |  |  |  |  |
|  | Is media containing information protected against unauthorized access, misuse or corruption during transportation? |  |  |  |  |  |  |
| 8.1 | Operational planning and control |  |  |  |  |  |  |
|  | Does the organization plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined from the opportunities and risk assessments? |  |  |  |  |  |  |
|  | Does the organization implement plans to achieve its information security objectives? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Does the organization keep documented information to the extent necessary to have confidence that the processes have been carried out as planned? |  |  |  |  |  |  |
|  | Does the organization control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary? |  |  |  |  |  |  |
|  | Does the organization ensure that outsourced processes are determined and controlled? |  |  |  |  |  |  |
| 8.2 | Information security risk assessment |  |  |  |  |  |  |
|  | Does the organization perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account additional risk assessment which may have been identified? |  |  |  |  |  |  |
|  | Does the organization retain documented information of the results of the information security risk assessments? |  |  |  |  |  |  |
| 8.3 | Information security risk treatment |  |  |  |  |  |  |
|  | Does the organization implement the information security risk treatment plan? |  |  |  |  |  |  |
|  | Does the organization retain documented information of the results of the information security risk treatment? |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 9 | Performance evaluation |  |  |  |  |  |  |
| 9.1 | Monitoring, measurement, analysis and evaluation |  |  |  |  |  |  |
|  | Does the organization evaluate the information security performance and the effectiveness of the information security management system? |  |  |  |  |  |  |
|  | Does the organization determine what needs to be monitored and measured, including information security processes and controls? |  |  |  |  |  |  |
|  | Does the organization determine the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results? |  |  |  |  |  |  |
|  | Does the organization determine when the monitoring and measuring shall be performed? |  |  |  |  |  |  |
|  | Does the organization determine when the results from monitoring and measurement shall be analysed and evaluated? |  |  |  |  |  |  |
|  | Does the organization determine who shall analyse and evaluate these results? |  |  |  |  |  |  |
|  | Does the organization retain appropriate documented information as evidence of the monitoring and measurement results? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 9.2 | Internal audit |  |  |  |  |  |  |
|  | Does the organization conduct internal audits at planned intervals to provide information on whetherthe information security management system conforms toits’ own and ISO 27001:2013 requirements for its information security management system? |  |  |  |  |  |  |
|  | Does the organization ensure that the requirements are effectively implemented and maintained? |  |  |  |  |  |  |
|  | Does the plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting? |  |  |  |  |  |  |
|  | Does the audit programme(s) take into consideration the importance of the processes concerned and the results of previous audits? |  |  |  |  |  |  |
|  | Does the audit programme(s) define the audit criteria and scope for each audit? |  |  |  |  |  |  |
|  | Does the audit programme(s) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process? |  |  |  |  |  |  |
|  | Does the audit programme(s) ensure that the results of the audits are reported to relevant management? |  |  |  |  |  |  |
|  | Does the audit programme(s) ensure the retention of documented information as evidence of the audit programme(s) and the audit results? |  |  |  |  |  |  |
| 9.3 | Management review |  |  |  |  |  |  |
|  | Do top management review the organization’s information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness? |  |  |  |  |  |  |
|  | Does the management review include consideration of:1. the status of actions from previous management reviews;
2. changes in external and internal issues that are relevant to the information security management system;
3. feedback on the information security performance, including trends in:
	* 1. nonconformities and corrective actions;
		2. monitoring and measurement results;
		3. audit results; and
		4. fulfilment of information security objectives;
4. feedback from interested parties;
5. results of risk assessment and status of risk treatment plan; and
6. opportunities for continual improvement.
 |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Do the outputs of the management review include decisions related to continual improvement opportunities and any needs for changes to the information security management system? |  |  |  |  |  |  |
|  | Does the organization retain documented information as evidence of the results of management reviews? |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | Improvement |  |  |  |  |  |  |
| 10.1 | Nonconformity and corrective action |  |  |  |  |  |  |
|  | When a nonconformity occurs, does the organization:1. react to the nonconformity, and as applicable:
	* 1. take action to control and correct it; and
		2. deal with the consequences;
2. evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur
3. or occur elsewhere, by:
	* 1. reviewing the nonconformity;
		2. determining the causes of the nonconformity; and
		3. determining if similar nonconformities exist, or could potentially occur;
4. implement any action needed;
5. review the effectiveness of any corrective action taken; and
6. make changes to the information security management system, if necessary.
 |  |  |  |  |  |  |
|  | Where corrective actions are taken are they appropriate to the effects of the nonconformities encountered? |  |  |  |  |  |  |
|  | Does the organization retain documented information as evidence of the nature of the nonconformities and any subsequent actions taken, and the results of any corrective action? |  |  |  |  |  |  |
| 10.2 | Continual improvement |  |  |  |  |  |  |
|  | Doe the organization continually improve the suitability, adequacy and effectiveness of the information security management system? |  |  |  |  |  |  |
|  | **Controls** |  |  |  |  |  |  |
|  | Has an access control policy been established, documented and reviewed based on business and information security requirements? |  |  |  |  |  |  |
|  | Are users only provided with access to the network and network services that they have been specifically authorized to use? |  |  |  |  |  |  |
|  | Has a formal user registration and de-registration process been implemented to enable assignment of access rights? |  |  |  |  |  |  |
|  | Is the allocation and use of privileged access rights restricted and controlled? |  |  |  |  |  |  |
|  | Is the allocation of secret authentication information controlled through a formal management process? |  |  |  |  |  |  |
|  | Do asset owners review users’ access rights at regular intervals? |  |  |  |  |  |  |
|  | Are the access rights of all employees and external party users to information and information processing facilities removed upon termination of their employment, contract or agreement, or adjusted upon change? |  |  |  |  |  |  |
|  | Are users required to follow the organization’s practices in the use of secret authentication information? |  |  |  |  |  |  |
|  | Is access to information and application system functions restricted in accordance with the access control policy? |  |  |  |  |  |  |
|  | Are password management systems interactive and ensure quality passwords? |  |  |  |  |  |  |
|  | Are the use of utility programs that might be capable of overriding system and application controls restricted and tightlyControlled? |  |  |  |  |  |  |
|  | Is access to program source code restricted? |  |  |  |  |  |  |
|  | Has a policy on the use of cryptographic controls for protection of information been developed and implemented? |  |  |  |  |  |  |
|  | Has a policy on the use, protection and lifetime of cryptographic keys been developed and implemented through their whole lifecycle? |  |  |  |  |  |  |
|  | Are security perimeters defined and used to protect areas that contain either sensitive or critical information and information processing facilities? |  |  |  |  |  |  |
|  | Are secure areas protected by appropriate entry controls to ensure that only authorized personnel are allowed access? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Have physical security for offices, rooms and facilities been designed and applied? |  |  |  |  |  |  |
|  | Has physical protection against natural disasters, malicious attack or accidents been designed and applied? |  |  |  |  |  |  |
|  | Have procedures for working in secure areas been designed andApplied? |  |  |  |  |  |  |
|  | Are access points such as delivery and loading areas and other points where unauthorized persons could enter the premises controlled and, if possible, isolated from information processing facilities to avoid unauthorized access? |  |  |  |  |  |  |
|  | Is equipment sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access? |  |  |  |  |  |  |
|  | Is equipment protected from power failures and other disruptions caused by failures in supporting utilities? |  |  |  |  |  |  |
|  | Is power and telecommunications cabling carrying data or supporting information services protected from interception, interference or damage? |  |  |  |  |  |  |
|  | Is equipment correctly maintained to ensure its continued availability and integrity? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Are procedures in place to ensure that equipment, information or software is not taken off-site without prior authorization? |  |  |  |  |  |  |
|  | Is security applied to off-site assets taking into account the different risks of working outside the organization’s premises? |  |  |  |  |  |  |
|  | Are all items of equipment containing storage media verifiedto ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use? |  |  |  |  |  |  |
|  | Do users ensure that unattended equipment has appropriate protection? |  |  |  |  |  |  |
|  | Has a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities been adopted? |  |  |  |  |  |  |
|  | Have operating procedures been documented and made available to all users who need them? |  |  |  |  |  |  |
|  | Are changes to the organization, business processes, information processing facilities and systems that affect information security controlled? |  |  |  |  |  |  |
|  | Is the use of resources monitored, tuned and projections made of future capacity requirements to ensure the required systemPerformance? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Are development, testing, and operational environments separated to reduce the risks of unauthorized access or changes to the operational environment? |  |  |  |  |  |  |
|  | Have detection, prevention and recovery controls to protect against malware been implemented, combined with appropriate user awareness? |  |  |  |  |  |  |
|  | Are backup copies of information, software and system images taken and tested regularly in accordance with an agreed backup policy? |  |  |  |  |  |  |
|  | Are event logs recording user activities, exceptions, faults and information security events produced, kept and regularlyReviewed? |  |  |  |  |  |  |
|  | Are logging facilities and log information protected against tampering and unauthorized access? |  |  |  |  |  |  |
|  | Are system administrator and system operator activities logged and the logs protected and regularly reviewed? |  |  |  |  |  |  |
|  | Are the clocks of all relevant information processing systems within an organization or security domain synchronised to a single reference time source? |  |  |  |  |  |  |
|  | Have procedures been implemented to control the installation of software on operational systems? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Is information about technical vulnerabilities of information systems being used to obtain in a timely fashion, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk? |  |  |  |  |  |  |
|  | Have rules governing the installation of software by users been established and implemented? |  |  |  |  |  |  |
|  | Are audit requirements and activities involving verification of operational systems carefully planned and agreed to minimise disruptions to business processes? |  |  |  |  |  |  |
|  | Are networks managed and controlled to protect information in systems and applications? |  |  |  |  |  |  |
|  | Are security mechanisms, service levels and management requirements of all network services identified and included in network services agreements, whether these services are provided in-house or outsourced? |  |  |  |  |  |  |
|  | Are groups of information services, users and information systems segregated on networks? |  |  |  |  |  |  |
|  | Are formal transfer policies, procedures and controls in place to protect the transfer of information through the use of all types of communication facilities? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Do agreements address the secure transfer of business information between the organization and external parties? |  |  |  |  |  |  |
|  | Is information involved in electronic messaging appropriately protected? |  |  |  |  |  |  |
|  | Are requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information identified, regularly reviewed and documented? |  |  |  |  |  |  |
|  | Is the information security related requirements included in the requirements for new information systems or enhancements to existing information systems? |  |  |  |  |  |  |
|  | Is information involved in application services passing over public networks protected from fraudulent activity, contract dispute and unauthorized disclosure and modification? |  |  |  |  |  |  |
|  | Is information involved in application service transactions protected to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay? |  |  |  |  |  |  |
|  | Have rules for the development of software and systems been established and applied to developments within the organization? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Are changes to systems within the development lifecycle controlled by the use of formal change control procedures? |  |  |  |  |  |  |
|  | When operating platforms are changed, are business critical applications reviewed and tested to ensure there is no adverse impact on organizational operations or security? |  |  |  |  |  |  |
|  | Are modifications to software packages discouraged, limited to necessary changes and all changes are strictly controlled? |  |  |  |  |  |  |
|  | Have principles for engineering secure systems been established, documented, maintained and applied to any information system implementation efforts? |  |  |  |  |  |  |
|  | Has the organizations established and appropriately protected secure development environments for system development and integration efforts that cover the entire system development lifecycle? |  |  |  |  |  |  |
|  | Does the organization supervise and monitor the activity of outsourced system development? |  |  |  |  |  |  |
|  | Is testing of security functionality carried out during development? |  |  |  |  |  |  |
|  | Have acceptance testing programs and related criteria been established for new information systems, upgrades and new versions? |  |  |  |  |  |  |
|  | Is test data selected carefully, protected and controlled? |  |  |  |  |  |  |
|  | Are information security requirements for mitigating the risks associated with supplier’s access to the organization’s assets agreed with the supplier and documented? |  |  |  |  |  |  |
|  | Are all relevant information security requirements established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization’s information? |  |  |  |  |  |  |
|  | Do agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain? |  |  |  |  |  |  |
|  | Does the organizations regularly monitor, review and audit supplier service delivery? |  |  |  |  |  |  |
|  | Are changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks? |  |  |  |  |  |  |
|  | Have management responsibilities and procedures been established to ensure a quick, effective and orderly response to information security incidents? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Are information security events reported through appropriate management channels as quickly as possible? |  |  |  |  |  |  |
|  | Are employees and contractors using the organization’s information systems and services required to note and report any observed or suspected information security weaknesses in systems or services? |  |  |  |  |  |  |
|  | Are information security events assessed and it shall be decided if they are to be classified as information security incidents? |  |  |  |  |  |  |
|  | Are information security incidents responded to in accordance with the documented procedures? |  |  |  |  |  |  |
|  | Is knowledge gained from analysing and resolving information security incidents used to reduce the likelihood or impact of future incidents? |  |  |  |  |  |  |
|  | Does the organization define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence? |  |  |  |  |  |  |
|  | Does the organization determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Has the organization established, documented, implemented and maintains processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation? |  |  |  |  |  |  |
|  | Does the organization verify the established and implementedinformation security continuity controls at regular intervals inorder to ensure that they are valid and effective during adverse situations? |  |  |  |  |  |  |
|  | Have information processing facilities been implemented with redundancy sufficient to meet availability requirements? |  |  |  |  |  |  |
|  | Are all relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements explicitly identified, documented and kept up to date for each information system and the organization? |  |  |  |  |  |  |
|  | Have appropriate procedures been implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products? |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Are records protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements? |  |  |  |  |  |  |
|  | Is privacy and protection of personally identifiable information ensured as required in relevant legislation and regulation where applicable? |  |  |  |  |  |  |
|  | Are cryptographic controls used in compliance with all relevant agreements, legislation and regulations? |  |  |  |  |  |  |
|  | Is the organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) reviewed independently at planned intervals or when significant changes occur? |  |  |  |  |  |  |
|  | Do managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements? |  |  |  |  |  |  |
|  | Are information systems regularly reviewed for compliance with the organization’s information security policies and standards? |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Has the client identified key performance or specific aspects, processes, operations and Operation of their Management System? |  |  |  |  |  |
|  |  |  |  |  |  |
| Have comments, observations, queries, NCR’s been issued to the client? |  |  |  |  |  |
| Scope of assessment applied for correct? |  |  |  |  |  |

CORRECTIVE ACTION / OPPORTUNITY FOR IMPROVEMENT REPORT

|  |  |
| --- | --- |
| OFI Ref No 1 |  |
| Notes |  |
| Area |  |
| Description of NCR |  |
| Category | Major / Minor / OFI |
| Standard |  |
| Clause |  |
| Response required by (dd/mm/yyyy) |  |
| Root cause of NCR and Client proposed actions |  |
| NCR Status |  |

CORRECTIVE ACTION / OPPORTUNITY FOR IMPROVEMENT REPORT

|  |  |
| --- | --- |
| OFI Ref No 2 |  |
| Notes |  |
| Area |  |
| Description of NCR |  |
| Category | Major / Minor / OFI |
| Standard |  |
| Clause |  |
| Response required by (dd/mm/yyyy) |  |
| Root cause of NCR and Client proposed actions |  |
| NCR Status |  |

CORRECTIVE ACTION / OPPORTUNITY FOR IMPROVEMENT REPORT

|  |  |
| --- | --- |
| NCR / OFI Ref No |  |
| Notes |  |
| Area |  |
| Description of NCR |  |
| Category | Major / Minor / OFI |
| Standard |  |
| Clause |  |
| Response required by (dd/mm/yyyy) |  |
| Root cause of NCR and Client proposed actions |  |
| NCR Status |  |

## Copy this page and create new pages if require